UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

ALICIA DAMON, individually and on behalf of all others similarly situated, Plaintiff, v. RECEIVABLES PERFORMANCE MANAGEMENT, LLC Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Alicia Damon, individually and on behalf of all others similarly situated ("Class Members"), brings this action against Receivables Performance Management, LLC ("RPM" or "Defendant"), and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Defendant is a large accounts receivable management company (i.e., a debt collector). In the ordinary course of business, Defendant acquires, processes, analyzes, and otherwise utilizes the personally identifiable information ("PII") of purported debtors, including, but not limited to, their names and Social Security numbers.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

2. Defendant failed to implement and maintain reasonable data security measures. As a result, on or about April 8, 2021, cybercriminals foreseeably accessed files on Defendant's network containing the PII of Plaintiff and millions of other Class Members. Defendant's monitoring practices were so poor that it did not identify this intrusion until May 12, 2021. It then reprehensibly waited until November 21, 2022 to begin notifying victims and the public of the Data Breach.

3. Defendant has disclosed that in total, the Data Breach impacted the PII of approximately 3,766,573 people.

4. While many details of the Data Breach remain in the exclusive control of Defendant, upon information and belief, Defendant breached its duties and obligations by failing to, in one or more of the following ways: (i) design, implement and maintain reasonable network safeguards against foreseeable threats; (ii) design, implement, and maintain reasonable data retention policies; (iii) adequately train employees on data security; (iv) comply with industry-standard data security practices; (v) warn Plaintiff and Class Members of Defendant's inadequate data security practices; (vi) encrypt or adequately encrypt the PII; (vii) recognize or detect that threat actors had accessed its network in a timely manner to mitigate the harm; (viii) utilize widely available software able to detect and prevent ransomware, and (ix) otherwise secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

5. As a result of Defendant's acts and omissions, Plaintiff and Class Members had Social Security numbers, their most sensitive PII, stolen by malicious cybercriminals. The information that was compromised is a one-stop shop for identity thieves to wreak havoc on

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiff's and Class Members' personal and financial lives. Given the sensitivity and static nature of the information involved, the risk of identity theft is present, materialized, and will continue into the foreseeable future for Plaintiff and Class Members. Plaintiff and Class Members will therefore now live with the present and ongoing risk of identity theft, which will require third-party professional services to monitor their PII for criminal misuse and dark web activity.

6. As a direct result of the Data Breach, Plaintiff and Class Members have suffered the following actual and imminent injuries: (i) invasion of privacy; (ii) out-of-pocket expenses; (iii) loss-of time and productivity incurred mitigating the present risk and imminent threat of identity theft; (iv) actual identity theft and fraud resulting in additional economic and non-economic damages; (v) diminution of value of their PII; (vi) anxiety, stress, nuisance, and annoyance; (vii) increased targeted and fraudulent robocalls and phishing email attempts; (viii) the present and continuing risk of identity theft posed by their PII being placed in the hands of the ill-intentioned hackers and/or criminals; (ix) the retention of the reasonable value of the PII entrusted to Defendant; and (x) the present and continued risk to PII, which remains on Defendant's vulnerable network, placing Plaintiff and Class Members at an ongoing risk of harm.

7. Plaintiff brings this class action to remedy these harms, on behalf of herself and all similarly situated persons whose PII was compromised in the Data Breach. Plaintiff seeks compensatory damages, incidental damages, and consequential damages for the diminution in value of hers and Class Members' PII, invasion of their privacy, loss of their time, loss of their productivity, out-of-pocket costs, and future costs of necessary identity theft monitoring. Plaintiff also seek injunctive relief including improvements to Defendant's data security system and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

protocols, deletion of PII that is unnecessary for legitimate business purposes, and future annual audits to protect their PII against foreseeable future cyber security incidents.

PARTIES

8. Plaintiff Alicia Damon is, and at all times mentioned herein was, an individual citizen of the State of New Jersey residing in the City of Middlesex. Plaintiff received a Notice of Data Security Incident Letter from Defendant dated November 21, 2022.

9. Defendant Receivables Performance Management is a corporation with its principal place of business located at 20818 44th Ave. W., Ste. 240, Lynnwood, WA 98036.

JURISDICTION AND VENUE

10. The Western District of Washington has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District, and Defendant conducts substantial business in Washington and in this District through its headquarters, offices, parents, and affiliates.

11. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000 exclusive of interest and costs; there are more than 100 members in the proposed class; and at least one member of the class, including the Plaintiff, is a citizen of a state different from Defendant.

12. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

BACKGROUND

13. Defendant claims that it is a "national leader in accounts receivable management."[1]

14. Defendant obtains the PII of Plaintiff and Class Members in order to provide debt collection services to its clients.

15. Defendant maintains a publicly available privacy policy ("Privacy Notice").[2] Due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to purported debtors, Defendant recognizes privacy rights, and promises in its Privacy Notice, to, among other things, maintain the privacy of individuals' PII and not disclose PII without authorization.

16. Plaintiff and the Class Members expected that Defendant would implement and maintain reasonable data security measures to protect their PII from foreseeable threats.

THE ATTACK AND DATA BREACH

17. On or about May 12, 2021, Defendant became aware of a data security incident that impacted its server infrastructure and took Defendant's system offline.[3] Defendant retained a forensic investigation firm that determined Defendant's systems were first accessed by cybercriminals on or about April 8, 2021. During this time, cybercriminals accessed and exfiltrated unencrypted files containing Plaintiff's and Class Members' PII, including Social Security numbers.

18. More than 3,700,000 victims were impacted by the Data Breach.[4]

---

[1] http://www.receivablesperformance.com/about-us.

[2] http://www.receivablesperformance.com/PrivacyPolicy.aspx.

[3] https://apps.web.maine.gov/online/aeviewer/ME/40/11ca5a7c-b09f-404a-81c6-b683305543a1.shtml (last visited November 29, 2022).

[4] *Id*.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

19. Based on its investigation, Defendant admits that Plaintiff's and Class Members' PII was accessed and exfiltrated via a ransomware attack conducted by cybercriminals.

20. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII of individuals like Plaintiff and the Class Members.

21. Due to Defendant's inadequate security measures, Plaintiff's and Class Members' PII is now in the hands of cyberthieves.

22. While Defendant stated in the Notice of Data Breach sent to Plaintiff and Class Members (as well as on its website) that it learned of the Data Breach on or around May 12, 2021, Defendant did not begin notifying impacted individuals, such as Plaintiff and Class Members, until November 21, 2022—over 18 months after first discovering the Data Breach.

The Data Breach was Foreseeable and Preventable

23. In 2021, a record 1,862 data breaches occurred, a 68% increase from 2020. Attacks involving ransomware—like the Data Breach here—are particularly on the rise, having doubled in each of the last two years.[5]

24. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller

[5] https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[6]

25. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

26. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures known to be generally effective at mitigating the risk of a cyberattack:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

[6] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Nov. 29, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[7]

27. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify

[7] *See* How to Protect Your Networks from RANSOMWARE, at 3–4, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Nov. 28, 2021).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

> website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .
>
> - **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
>
> - **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it. . . .
>
> - **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
>
> - **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
>
> - **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .[8]

28. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure internet-facing assets**
>
> - Apply latest security updates

[8] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Nov. 28, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[9]

29. Even if the cybercriminals had been able to access Defendant's network despite reasonable security measures, Defendant could have prevented the consequences by properly encrypting the files containing PII or destroying PII it no longer had a legitimate need for.

[9] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 28, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

30. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

31. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the unauthorized exposure and exfiltration of the PII of Plaintiff and Class Members.

Value of PII

32. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[10] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[11]

33. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit

[10] 17 C.F.R. § 248.201 (2013).

[11] *Id.*

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Nov. 28, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

card number can sell for $5 to $110 on the dark web.[13] Criminals can also purchase access to entire company data breaches for prices ranging from $900 to $4,500.[14]

34. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[15] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.16 Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[17]

35. The integrity of PII gives it its value because PII is used to secure loans, open lines of credit, verify identities, and unlock government benefits. When PII is used to commit fraud, these simple everyday necessities become more difficult, if not impossible, due to lowered credit scores and tarnished credit histories from credit fraud and identity theft.[18]

36. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals and is likely already available on the dark web due to its high

---

[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Nov. 28, 2022).

[14] *In the Dark*, VPNOverview, 2019, *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Nov. 28, 2022).

[15] *Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, Los Angeles Times, Nov. 5, 2019, *available at* https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[16] *See* https://datacoup.com/ and https://worlddataexchange.com/about.

[17] *Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Nov. 29, 2022).

[18] *The Negative Effects of Identity Theft*, LifeLock by Norton, *available at* https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft (last visited Nov. 29, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

value for threat actors. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss.

37. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[19]

38. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

39. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[20]

---

[19] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 28, 2022).

[20] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Nov. 28, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

40. Based on the foregoing, the PII compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The PII compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change: Social Security number and name.

41. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[21]

42. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing, or even give false information to police.

43. The fraudulent activity resulting from the Data Breach may not come to light for years.

44. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

---

[21] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at* https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Nov. 28, 2022).

[22] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited Nov. 28, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

45. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

46. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages, in addition to any fraudulent use of their PII.

47. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially millions of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

Defendant Failed to Comply with FTC Guidelines

48. Defendant was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

49. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[23]

50. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[24] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

51. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[25]

52. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

---

[23] FEDERAL TRADE COMMISSION, *Start With Security: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Nov. 28, 2022).

[24] FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 28, 2022).

[25] FTC, *Start With Security*, *supra*.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

53. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

54. Defendant was at all times fully aware of its obligation to protect the PII stored within its systems. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Plaintiff Damon's Experience

55. Plaintiff Damon is very careful with her PII. She stores any documents containing PII in a safe and secure location or destroys the documents. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. When Plaintiff does entrust a third-party with her PII, it is only because she understands the PII will be safeguarded in accordance with applicable privacy policies and state and federal law.

56. Plaintiff Damon provided PII, including her Social Security number, to one of Defendant's clients as a condition of receiving services. Upon information and belief, Defendant thereafter acquired this PII and used it when attempting to collect a purported debt.

57. Plaintiff received a letter from Defendant dated November 21, 2022 informing Plaintiff that her "personal information. . ., including Social Security number," were included in

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

files compromised during the Data Breach. To the best of Plaintiff's knowledge, this is the only letter she has ever received notifying her that her PII was compromised.

58. Plaintiff spent time researching the Data Breach to better understand what happened and to verify the legitimacy of the letter she received. Furthermore, Plaintiff has spent (and will continue to spend) considerable time exploring credit monitoring and identity theft protection services and self-monitoring her accounts and credit reports.

59. Plaintiff also experienced actual injury in the form of fraudulent activity on her financial accounts. First, in approximately December 2021, Plaintiff experienced multiple fraudulent charges on her Wells Fargo debit card. The card had to be cancelled and reissued. It took the bank several days to refund the fraudulent purchases, during which time Plaintiff was without the use of these funds. The fraudulent charges caused Plaintiff's account to decline below $0, causing her to incur overdraft fees. Plaintiff also incurred late fees and/or service fees as a result of missed automatic bill payments scheduled to taken from the cancelled account. None of the fees Plaintiff incurred have been refunded.

60. Next, in early 2022, Plaintiff experienced fraudulent charges on her CashApp debit card. The card had to be cancelled and reissued. It took several days to refund the fraudulent purchases, during which time Plaintiff was without the use of these funds. Plaintiff also incurred late fees and/or service fees as a result of missed automatic bill payments scheduled to taken from the cancelled account. These fees have not been refunded.

61. In approximately September 2022, Plaintiff received a suspicious call from an individual purporting to be from CashApp. In an apparent effort to gain Plaintiff's trust, the caller recounted personal and financial information about Plaintiff that should have been private. The

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

caller then requested that Plaintiff provide him with information about Plaintiff's Wells Fargo account. When Plaintiff engaged in further questioning of the caller, he hung up.

62. In October 2022, Plaintiff received a copy of her records from the IRS. She did not request these records, which included all of her private tax filing information dating back to 2018. Upon information and belief, an unauthorized individual requested these records from the IRS on Plaintiff's behalf.

63. Plaintiff has suffered lost time, annoyance, interference, and inconvenience dealing with the aforementioned consequences of the Data Breach and has anxiety over the present risk of harm she faces and the loss of her privacy that has already occurred.

64. Plaintiff has suffered injury from the substantial risk of imminent and impending fraud, theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in revealing the true nature of the threat to Plaintiff's PII.

65. Upon information and belief, Defendant continues to maintain Plaintiff's PII in an unsecured manner on its network despite not having a legitimate need for it. Plaintiff has a continuing interest in ensuring that her PII is protected and safeguarded from future breaches.

Plaintiff's and Class Members' Harms and Damages

66. Defendant has done little to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in the Data breach. Defendant's Notice of Data Breach completely downplays and disavows the theft of Plaintiff's and Class Members' PII, when the facts demonstrate that the PII was accessed and exfiltrated. The complimentary fraud and identity

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

monitoring service offered by Defendant is inadequate, as the services are offered for only 12 months and require Plaintiff and Class Members to spend time signing up.

67. Plaintiff and Class Members have been injured and damaged by the compromise of their PII in the Data Breach.

68. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, and similar identity theft.

69. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

70. Plaintiff and Class Members will also incur out-of-pocket costs for protective measures such as credit monitoring fees (for any credit monitoring obtained in addition to or in lieu of the inadequate monitoring offered by Defendant), credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

71. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by the hacker and cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

72. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

73. Plaintiff and Class Members have and/or will suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

a. Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Closely reviewing and monitoring Social Security Numbers, bank accounts, and credit reports for unauthorized activity for years to come.

74. Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing sensitive and confidential personal, health, and/or financial information is not accessible online, that access to such data is password-protected, that such data is properly encrypted, and that such data is not stored for longer than Defendant has a legitimate need.

75. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

76. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

CLASS REPRESENTATION ALLEGATIONS

77. Plaintiff brings this nationwide class action on behalf of herself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

78. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All United States residents whose PII was accessed or acquired during the data breach event that is the subject of the Notice of Data Breach letter that Defendant sent to Plaintiff and other Class Members on or around November 21, 2022 (the "Nationwide Class").

79. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

80. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") is so numerous that joinder of all members is impracticable. Defendant has identified millions of individuals whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records. Defendant advised the Office of the Maine Attorney General that the Data Breach affected more than 3,700,000 individuals.

81. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the hacking incident and Data Breach;

c. Whether Defendant's data security systems prior to and during the hacking incident and Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether computer hackers obtained Class Members' PII in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Defendant owed a duty to provide Plaintiff and Class Members notice of this Data Breach, and whether Defendant breached that duty to provide timely notice;

j. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct violated federal law;

m. Whether Defendant's conduct violated state law;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or punitive damages.

82. Common sources of evidence may also be used to demonstrate Defendant's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Defendant's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

83. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach and due to Defendant's misfeasance.

84. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

85. Predominance, Fed. R. Civ. P. 23 (b)(3). Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

86. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

87. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged. Absent class treatment, Defendant would necessarily gain an unconscionable advantage because it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

88. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

89. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

90. Unless a class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

91. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

92. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

93. Defendant acted on grounds that apply generally to the Class as a whole, so that Class certification and the corresponding relief sought are appropriate on a Class-wide basis.

Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

FIRST COUNT
Violation of the Washington State Consumer Protection Act
(RCW 19.86.010 *et seq*.)
(On Behalf of Plaintiff and the Nationwide Class)

94. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

95. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce.

96. Defendant is a "person" as described in RCW 19.86.010(1).

97. Defendant engages in "trade" and "commerce" as described in RCW 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

98. Defendant is headquartered in Washington; its strategies, decision-making, and commercial transactions originate in Washington; most of its key operations and employees reside, work, and make company decisions (including data security decisions) in Washington; and Defendant and many of its employees are part of the people of the State of Washington.

99. In the course of conducting its business, Defendant committed "unfair acts or practices" by, among other things, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's unfair acts and practices are ongoing and continue to this date.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

100. Defendant's conduct was also deceptive. Defendant failed to timely notify and concealed from Plaintiff and Class Members the unauthorized release and disclosure of their PII. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII and identities.

101. Defendant's above-described "unfair or deceptive acts or practices" in violation of the CPA affects the public interest because it is substantially injurious to persons, had the capacity to injure other persons, and has the capacity to injure other persons.

102. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

103. Defendant's above-described unfair and deceptive acts and practices directly and proximately caused injury to Plaintiff and Class Members' business and property. Plaintiff and Class Members have suffered, and will continue to suffer, actual damages and injury in the form of, among other things, (1) an imminent, immediate, and continued increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which he or she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of his or her PII; (5) deprivation of the value of his or her PII, for which there is a well-established national and international market; (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages; and/or (7) investment of substantial time and money to monitor and remediate the harm inflicted upon them.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

104. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct, and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect PII .

105. Plaintiff, on behalf of Plaintiff and the Class Members, also seeks to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiff, on behalf of Plaintiff and the Class Members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained, not to exceed $25,000.00 per class member.

SECOND COUNT
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

106. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

107. Plaintiff brings this claim individually and on behalf of the Class.

108. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

109. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' PII within its possession was compromised and precisely the type(s) of information that were compromised.

110. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

111. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

112. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Class Members, which is recognized by laws and regulations, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

113. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

114. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

115. Defendant systematically failed to provide adequate security for data in its possession.

116. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Upon information and belief, mishandling emails, so as to allow for unauthorized person(s) to access Plaintiff's and Class Members' PII;

b. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

c. Failing to adequately monitor the security of its networks and systems;

d. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

117. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within Defendant's possession.

118. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

119. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

120. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII would result in injury to Plaintiff and Class Members.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

121. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII would result in injuries to Plaintiff and Class Members.

122. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

123. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members regarding what type of PII has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

124. Defendant's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their PII.

125. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

126. Plaintiff seeks the award of actual damages on behalf of the Class. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to PII; and (2) compelling Defendant to provide detailed and specific disclosure of what types of PII have been compromised as a result of the Data Breach.

THIRD COUNT
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class)

127. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

128. At all times during Defendant's possession of Plaintiff's and the Class Members' PII, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Class Members' PII.

129. Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and the Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

130. Defendant voluntarily received in confidence Plaintiff's and the Class Members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

131. Due to Defendant's failure to prevent the Data Breach from occurring, Plaintiff's and the Class Members' PII was disclosed to and misappropriated by unauthorized third parties beyond Plaintiff's and the Class Members' confidence, and without their express permission.

132. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

133. But for Defendant's disclosure of Plaintiff's and the Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and the Class Members' PII as well as the resulting damages.

134. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Class Members' PII. Defendant knew or should have known its methods of accepting and securing Plaintiff's and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

the Class Members' PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Class Members' PII.

135. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention of, detection of, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact on the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

136. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for relief as follows:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees'

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years,

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

D. For an award of damages, including, but not limited to, actual, consequential, nominal, and treble damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

Dated: November 29, 2022

TOUSLEY BRAIN STEPHENS PLLC

By: *s/ Jason T. Dennett*
s/ Kaleigh N. Boyd

Jason T. Dennett, WSBA #30686
Kaleigh N. Boyd, WSBA #52684
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101-3147
Tel: (206) 682-5600/Fax: (206) 682-2992
jdennett@tousley.com
kboyd@tousley.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Tel: (513) 651-3700/Fax: (513) 665-0219
tcoates@msdlegal.com/
dgould@msdlegal.com

**Pro Hac Vice Application forthcoming*
Counsel for Plaintiff and Putative Class Members

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992